APAC
ASIA PACIFIC
ACCREDITATION COOPERATION
Competence | Acceptance | Equivalence

ACCREDITATION: BUILDING TRUST IN INFORMATION SECURITY

secretariat@apac-accreditation.org

www.apac-accreditation.org

+61 466 262 372

PO Box 5154 South Turramurra
NSW 2074 Australia

APAC
ASIA PACIFIC ACCREDITATION COOPERATION
Competence | Acceptance | Equivalence

ACCREDITATION: Building Trust in Information Security

Information security protects and prevents unauthorized access, use, disclosure, disruption, modification or destruction of data and information, especially in electronic information management and cyberspace. Organizations, customers and consumers need to have confidence that their data is securely managed, and any risks are being effectively managed.

ISO/IEC 27001 is the leading international standard for information security management which defines the requirements of an information security management system (ISMS). This standard outlines a risk management process involving people, processes and IT systems, thereby providing a holistic approach to information security. This international standard is adopted by organizations of all sizes around the world, and helps them gain acceptance for their ISMS on a global scale.

APAC
ASIA PACIFIC
ACCREDITATION COOPERATION
Competence | Acceptance | Equivalence

FEATURES OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

- Assists organisations in establishing policies and objectives about information security management and implementing controls to manage security of information
- Assists organizations to manage its regulatory obligations in conjunction with ISO/IEC 27701 and to regularly check the compliance status
- The scope covers information security generally and not only information technology security
- Adopts the Plan-Do-Check-Act (PDCA) model and uses a process approach to establish, implement, operate, monitor, review, maintain and improve Information security
- Focuses on people, processes and technology
- Utilises a combination of objectives, management controls, operational controls and technical controls
- Continual improvement of the system to ensure protection and address vulnerabilities before they arise
- Allows for business controls and management processes that are proportionate to the nature and type of information security threats and opportunities

APAC
ASIA PACIFIC ACCREDITATION COOPERATION
Competence | Acceptance | Equivalence

BENEFITS OF IMPLEMENTING AN ISMS

THE BENEFITS OF IMPLEMENTING AN ISMS INCLUDE:

- Protection of confidential information
- Allowing only authorized persons to access information
- Establish an independent framework that takes into account legal and regulatory requirements
- Security of information assets
- Risk analysis and resilience of information security
- Ensures integrity of business data and completeness of information and processing methods
- Provides comprehensive approach to information security
- Demonstrating senior management commitment to the security of business information and customer information
- Safeguarding of third-party information
- Aligning the processes with international standards thereby preventing disruptions to critical processes and preventing financial losses

APAC
ASIA PACIFIC ACCREDITATION COOPERATION
Competence | Acceptance | Equivalence

BENEFITS OF IMPLEMENTING AN ISMS

THE BENEFITS OF IMPLEMENTING AN ISMS INCLUDE:

- Gaining trust and confidence amongst regulators and customers
- Prevention, preparedness and protection against computer fraud, loss of data
- Reduces risk and costs associated with data/security breaches
- Formalizes and verifies, information security processes, procedures and documentation
- Adopts a process-based approach for implementing, establishing, monitoring, operating, maintaining, and improving your information security management system
- Gives the ability to demonstrate and independently assure the internal controls of a organization (corporate governance)
- Provides a competitive edge to the company, strengthens customer confidence and corporate brand
- Drives improvement in strategies, processes and performance
- Protects the organization's supply chain security
- Implementation of best practices

GLOBAL ACCEPTANCE OF ISMS CERTIFICATES

Accreditation bodies that are signatories to the Asia Pacific Accreditation Cooperation (APAC) Mutual Recognition Arrangement (MRA) and the International Accreditation Forum (IAF) Multilateral Arrangement (IAF MLA) recognise the accredited certificates by all other signatories. This means that an accredited ISMS certificate for an organization in one economy can be accepted by organizations in other economies. This facilitates trust amongst businesses, trading partners, global supply chains, and with regulators and consumers.

Under accredited ISMS certification the following requirements are fulfilled:

1. ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
2. ISO/IEC 27006 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems (including amendments)
3. IAF requirements
4. APAC requirements

Using accredited ISMS certification is a market differentiator and demonstrates an organisation's commitment and capability to implementing a secure ISMS that keeps information assets secure and mitigates risks.

What is APAC?

The Asia Pacific Accreditation Cooperation (APAC) is an association of accreditation bodies from the Asia Pacific region. It was established on 1 January 2019 with the amalgamation of two former regional accreditation cooperation - the Asia Pacific Laboratory Accreditation Cooperation (APLAC) and the Pacific Accreditation Cooperation (PAC).

To know about Asia Pacific Accreditation Cooperation (APAC), please click here